Computer and Network Access Requirements for Users and Equipment

1. Compliance with the instructions listed below is mandatory when performance under this contract requires access to Air Force unclassified computer systems or networks (stand alone or networked) and/or when contractor-owned Automated Data Processing Equipment (ADPE) will be used to access Air Force unclassified computer systems or networks (stand alone or networked).

--Air Force Instruction (AFI) 31-501, Personnel Security Program Management
--AFI 33-115, Network Management and Licensing Network Users and Certifying Network Professionals
--AFI 33-119, Electronic Mail (E-mail) Management and Use
--AFI 33-202, Computer Security
--AFI 33-204, Information Protection Security Awareness, Training, and Education (SATE)
--AFMAN 33-223, Identification and Authentication
--AFMC Supplement 1, AFMAN 33-223, Identification and Authentication
--DoD 5200.2-R, Personnel Security Program

2. Contractors requiring access to the Air Force Research Laboratory Propulsion Directorate (AFRL/PR) unclassified computer systems or networks for their employees and/or contractor owned ADPE shall comply with specific network access requirements and ADPE restrictions outlined below.

a. ADPE Restrictions

(1) All Contractor-owned ADPE shall be certified and accredited by the Designated Approval Authority (DAA), the Director of AFRL/PR, or the Deputy Director of AFRL/PR, if the Director is absent, ***before*** it is granted authorization to be connected as a stand-alone system, or connected directly to an AFRL/PR network. Deviation from this requirement may result in contractor ADPE being removed from the AFRL/PR network.

(2) The Contractor shall contact the Chief Technology Officer, AFRL/PROE, (937) 255-2319, when contractor-owned ADPE is to be connected to the AFRL/PR network. This point of contact will verify that all contractor-owned ADPE meets minimum security baselines and that it is certified and accredited before network connectivity is granted. The Government will prepare the certification and accreditation documentation with input and cooperation from the Contractor.

(3) Once certified, contractor-owned ADPE shall be maintained at the required security level by following all Air Force Information Assurance (IA) procedures. This includes:

(a) Establishing timelines to install all required security patches, anti-virus software, Time Compliance Network Orders (TCNOs) and Notice to AirMan (NOTAMs). (NOTAMs and TCNOs are security directives from the Network Operations and Security Center (AFMC/NOSC).) NOTAMS and TCNOs will be provided to the Contractor System Administrator by the appropriate AFRL/PR IA focal point.

(b) Installing all Air Force or AFMC mandated software to contractor owned ADPE connected to the network.

(c) Installing anti-virus software and ensuring it is executed daily on every device. As an alternative, the anti-virus software shall have real-time protection enabled.

(4) The Contractor shall contact the COMPUSEC manager, AFRL/PROE, (937) 255-2054, when software or hardware modifications are made so that government system documentation can be updated. Depending upon the degree of modification(s), the COMPUSEC manager reserves the right to reassess the ADPE for compliance.

b. Network Access Requirements

(1) The Contractor shall submit a request for access to the AFRL/PR network to AFRL/PROB Security Specialist, (937) 254-8609 for each of the contractor's employees, representatives and subcontractor employees who require access to Air Force unclassified computer systems or networks. This request shall include a System Access Request (SAR) Form (AFRL Form 25). Prior to final approval of the SAR, either clearance information or a favorable National Agency Check (NAC) is required in accordance with DoD 5200.2-R.

(2) If the Contractor's employees, representatives or subcontractor employees do not have a NAC, a completed Electronic Personnel Security Questionnaire (EPSQ), SF85P, Questionnaire for Public Trust Position and DD Form 258, Fingerprint Card must be submitted to AFRL/PROB. (The SF85P can be found at http://www.dss.mil. The 88th Security Forces Squadron (SFS) personnel will fingerprint the contractor employees.)

(3) Each Contractor employee, representative, and subcontractor employee requiring access to Air Force unclassified computer systems or networks shall complete Security Awareness, Training and Education (SATE) training and submit documentation of completion to AFRL/PROE before final processing of the SAR.

3. Interim Access

a. Interim access may be granted to the contractor employee provided that:

(1) Access to an unclassified government automated information system (AIS) or e-mail account is required for performance of the contractual effort.

(2) The contractor employee has completed and submitted the EPSQ (SF85P) to the AFRL/PR Security Specialist or SF 86 to the contractor facility security officer (FSO). The FSO shall verify, in writing, the action to the AFRL/PR Security Specialist.

(3) SATE training has been completed and verification has been submitted to AFRL/PROE.

(4) The SAR form (AFRL Form 25) has been completed with all appropriate signatures, and has been submitted to AFRL/PROE.

(5) The DAA has signed a letter approving interim access

b. The DAA may withdraw access to Government automated information systems if the completed NAC identifies information that is determined to be disqualifying.

4. Foreign Nationals -- HQ AFMC/CV approval is required for network connectivity or access to a Government system by foreign nationals. Foreign nationals shall not be authorized interim access to unclassified government automated information systems.

5. Account Revalidation -- Each contractor employee, representative, or subcontractor employee authorized user shall revalidate their account information yearly. AFRL/PROE will provide instructions to all users, directing them to the appropriate web location containing forms and instructions. A compliance suspense date will be established. Accounts that are not revalidated after the established suspense date shall be disabled.

6. System Administrator

a. A System Administrator is defined as the individual operationally and administratively responsible for the proper functioning of the stand-alone or multi-user system typically having root or system administrator operator privileges. The system administrator resolves the day-to-day administrative and technical system problems. Contractor employees administering a computer system or network are, by definition, system administrators.

b. Contractor system administrators shall follow Air Force Systems Security Instruction (AFSSI) 5027, Network Security Policy, and all Air Force IA procedures, including installing all required security patches, TCNOs and NOTAMs, and report feedback information to the appropriate AFRL/PR IA focal point.

c. Contract system administrators are required to monitor log files and report any suspicious activity to the Information System Security Officer (ISSO), AFRL/PROE, (937) 255-2416.

d. All contractor system administrators are required to complete annual Air Force provided security training.